NUI Galway
OÉ Gaillimh

Autumn Examinations 2017/2018

Exam Code(s)	4BCT1, 1MECE1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	Yes
External Examiner(s)	Dr. Jacob Howe
Internal Examiner(s)	Prof. M. Madden *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	X	No	
MCQ	Yes		No	X
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes		No	X

PTO

1 (a) Explain what is meant by the term 'nonce', and show how a nonce can be used to provide evidence of freshness in a communication (9 marks)

(b) Outline how any one dynamic password scheme (e.g. token-based challenge response) that you are familiar with can be used to provide evidence of identity in a communication (8 marks)

(c) Your organisation is considering moving to a two-factor authentication scheme. Currently authentication is achieved via usernames and passwords that must be at least five characters long. From a security perspective, would this proposed move be a good idea in your view? (8 marks)

2 (a) List any three criteria that a forensic investigative technique should satisfy in order to have confidence that evidence supplied by the investigative technique is reliable. (8 marks)

(b) Does steganographic software provide any special difficulties for digital forensic investigations in your view?(9 marks)

(c) Outline any two challenges that you think face digital forensics through the emergence of mobile devices (8 marks)

3
Consider the document 'Framework for Improving Critical Infrastructure Cybersecurity', released by the National Institute of Standards and Technology (NIST) as draft version 1.1 in January 2017. The framework presented in this document is, as stated in the document, a 'risk-based approach to managing cybersecurity risk'. Give your understanding of this framework under the three headings 'Framework Core' (9 marks), 'Framework Implementation Tiers' (8 marks) and 'Framework Profile' (8 marks).

4 (a) Give any one security property that a cryptographic hash function should satisfy, and briefly indicate one application area where in your view this security property is needed (9 marks)

(b) What does a message authentication code (MAC) offer that a hash function does not? (8 marks)

(c) Sketch how a MAC scheme can provide a non-repudiation service, assuming the existence of a trusted third party (arbitrator) (8 marks)

5 (a) By considering the plaintext ‘011100’ and an associated key ‘000000’, explain the principle underlying encryption and decryption for a simple stream cipher that depends on a randomly generated keystream and XOR (8 marks)

(b) ‘Block ciphers work on blocks rather than bits’. With the aid of a diagram, show one encryption round for the AES block cipher (8 marks)

(c) Outline what is meant by a Message Authentication Code (MAC) forgery attack. Assume that the same key has been used for a confidentiality service and an integrity service, and that both services are provided by a Cipher Block Chain (CBC) scheme. (9 marks)

6 (a) In the context of a public key encryption scheme such as RSA, explain what is meant by the terms ‘Registration Authority’ and ‘Digital Certificate’ (8 marks)

(b) Outline how an RSA digital signature scheme works (9 marks)

(c) Explain in your own words what is meant by the idea that public key encryption and public key digital signature have complementary requirements. (8 marks)